Docket No.: 03226/475001; P8956
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Wei Sun et al.

Application No.: 10/683,728

Filed: October 9, 2003

For: METHOD AND SYSTEM FOR TRANSFERRING IDENTITY ASSERTION INFORMATION BETWEEN TRUSTED PARTNER SITES IN A NETWORK USING ARTIFACTS

Confirmation No.: 1630

Art Unit: 2436

Examiner: C. C. Okoronkwo

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

As required under § 41.37(a), this brief is filed within two months of the Notice of Appeal filed in this case on December 8, 2008, and is in furtherance of said Notice of Appeal.

TABLE OF CONTENTS

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1205.2:

TABLE OF AUTHORITIES

A. Court and Administrative Decisions

B. Statutes

C. Other Authorities

I. REAL PARTY IN INTEREST

The real party in interest for the referenced application is Sun Microsystems, Inc. An Assignment transferring all interest in the referenced application from the inventors to Sun Microsystems, Inc. was filed with the USPTO on October 3, 2003. The Assignment is recorded at Reel 014592, Frame 0391.

I. STATEMENT OF RELATED CASES

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

II. JURISDICTIONAL STATEMENT

The Board has jurisdiction under 35 U.S.C. §134(a). The Examiner mailed a final rejection on October 17, 2008 ("Final Rejection"), setting a three-month shortened statutory period for response. The time for responding to the final rejection expired on January 17, 2009. Rule 134. A notice of appeal was filed on December 8, 2008. The time for filing an appeal brief is two months after the filing of a notice of appeal. Bd. R. 41.37(c). The time for filing an appeal brief expires on February 8, 2008. The appeal brief is being filed on February 6, 2009.

III. STATUS OF AMENDMENTS

Appellant filed an Amendment on January 2, 2009 in response to the Final Office Action. These amendments have been entered and considered by the Examiner. The pending claims of record are presented in the Claims Appendix.

IV. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The rejections to be reviewed on this appeal include the rejection of claims 27-31, 33-35, 37-38, 40-45, and 47 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 7,010,582 ("Cheng") and the rejection of claims 32, 36, 39, and 46 as being unpatentable under 35 U.S.C. §103(a) over Cheng in view of U.S. Patent Publication No. 2003/0177388 ("Botz").

V. STATEMENT OF FACTS

Claims 27-31, 33-35, 37-38, 40-45, and 47 have been rejected by the Examiner under 35 U.S.C. §102(e) as being anticipated by Cheng. Claims 32, 36, 39, and 46 have been rejected by the Examiner as being unpatentable over Cheng in view of Botz.

Briefly, claim 27 of the invention is directed to a method for managing access to a plurality of applications using a central server. In particular, independent claim 27 requires, in part, (i) authenticating a user using a user name and password to a first application; (ii) in response to the successful authentication, generating identity assertion information for use by a plurality of applications to authenticate the user; (iii) providing the first application with a first artifact, where the first artifact is used to obtain the identity assertion information; (iv) providing the first artifact to a second application, where the second application uses the first artifact to obtain the identity assertion information; (v) authenticating the user using the identity assertion information to the second application; (vi) generating a second artifact, where the first artifact is used to obtain the identity assertion information (*i.e.,* the same identity assertion information mentioned in (iii)); and (vii) rendering the first artifact invalid for future use by any of the plurality of applications.

Briefly, Cheng discloses a system and method for providing access control information from a first server to a second server through an end user device. *See* Cheng col. 2, ll. 5-8. An end user device sends a message to the first network device. In response, the first network device sends a response message to the user device including access control information to be conveyed to the second network device, as well as instructions to send the access control information to the second

network device. *See* Cheng, col. 2, ll. 13-20. When a request is sent to the first network device, such as a multiple domain, single sign on (MDSSO) server, the MDSSO server generates an MDSSO cookie and sends the cookie back to the user device. The cookie is valid at each domain in an MDSSO group. *See* Cheng, col. 6, ll. 53-64.

In rejecting claim 27, the Examiner contends that Cheng discloses sending the first artifact to the first application in col. 1, ll. 52-60. The Examiner contends that sending the first artifact to an application is identical to "sending credit card information, street address, telephone number, social security number, bank details, personal health information, taxation data, criminal records … from one server to another." *See* Final Rejection p. 5. Accordingly, the examiner contends that the credit card information, street address, etc. are identical to the first artifact. The cited section of Cheng discloses "sending credit card information, street address, telephone number … from one server to another may be a violation of privacy laws." *See* Cheng col. 1, ll. 52-60.

Further in rejecting claim 27, the Examiner contends that Cheng discloses rendering the first artifact invalid for future use, after the first use, by any of the plurality of applications in col. 7, ll. 9-11. *See* Final Rejection p. 7. This section of Cheng discloses that the cookie may have an expry date. *See* Cheng col. 7, ll. 9-

11. Accordingly, the Examiner contends that the first artifact of the claimed invention is identical to the cookie of Cheng.

The Examiner also contends that Cheng discloses receiving a request for a second artifact from the second application in col. 10, ll. 42-46. *See* Final Rejection p. 7. This section of Cheng discloses sending a request to a second server, where the request includes data to be transferred from a first server to the second server. *See* Cheng col. 10, ll. 42-46. Accordingly, the Examiner contends that the data to be transferred in Cheng is identical to the second artifact of the claimed invention.

Briefly, Botz discloses an authentication identity translation technique that facilitates signing on in a computer environment including multiple servers, such that an authenticated user identification on a first server is translated to an associated local identity on another server in the environment. *See* Botz para. [0028].

VI. ARGUMENT

In this Appeal, the Appellants assert that the Examiner erred in contending that claims 27-31, 33-35, 37-38, 40-45, and 47 are anticipated under 35 U.S.C. § 102(e) over Cheng for at least the reasons stated below. For the purposes of this Appeal, claims 27-31, 33-35, 37-38, 40-45, and 47 stand or fall together.

Independent claim 27 is representative of the group including claims 27-31, 33-35, 37-38, 40-45, and 47.

Further in this Appeal, the Appellants assert that the Examiner erred in contending that claims 32, 36, 39, and 46 are unpatentable under 35 U.S.C. § 103(a) over Cheng and in view of Botz, viewed separately or in combination, for at least the reasons stated below. For the purposes of this Appeal, claim 32 is representative of the group including claims 32, 36, 39, and 36.

A. **Claim 27**

In this Appeal, the Appellants argue that claims 27-31, 33-35, 37-38, 40-45, and 47 are not anticipated under 35 U.S.C. § 102(e) over Cheng for at least the reasons stated below. Specifically, the Examiner at least erroneously contends that Cheng discloses: i) generating and sending a first artifact associated with the identity assertion information, wherein the first artifact is used to obtain the identity assertion information; ii) verifying the validity of the first artifact upon receipt from the second application; and iii) rendering the first artifact invalid for future use by any of the plurality of applications.

1. Cheng fails to disclose generating a first artifact associated with the identity assertion information, wherein the first artifact is used to obtain the identity assertion information.

Variations of this argument were presented in the responses filed on February 26, 2008, June 27, 2008, and January 2, 2009. Claim 27 requires, in part, i) generating a first artifact, wherein the first artifact is associated with identity assertion information (data associated with a user); and ii) using the first artifact to obtain the identity assertion information. Appellants assert that Cheng fails to meet at least these two requirements regarding the first artifact.

The Examiner contends that Cheng discloses generating a first artifact associated with identity assertion information in col. 1, ll. 52-60, where the first artifact is identical to "credit card information, street address, telephone number, social security number, bank details, personal health information, taxation data, criminal records." *See* Final Rejection p. 5. Accordingly, the Examiner contends that the first artifact is identical to the credit card information, street address, etc. of Cheng.

In order for prior art to anticipate a claim, the identical invention must be shown in the prior art. In *Richardson v. Suzuki* ("*Richardson*"), the United States Court of Appeals for the Federal Circuit held that "[t]he identical invention must be shown in as complete detail as is contained in the claim." *Richardson v. Suzuki*

Motor Co., 868 F.2d 1226, 1236 (Fed. Cir. 1989). By way of analogy, the invention in *Richardson* was a modified suspension system for a motorcycle that would provide a smooth ride over rough terrain. The invention was, generally, a "system consisting of a single shock absorber plus a linkage consisting of a bell crank and connecting rod. This linkage generated a 'rising rate'..." *Id.* Suzuki, claiming invalidity of the Richardson patent, relied on several pieces of prior art, each as anticipating the Richardson invention. One of the patents that Suzuki cited as anticipating the Richardson invention was the Downs reference. The Downs reference disclosed a suspension that had a "spring element that is rigidly attached to the motorcycle frame and does not pivot." *Id.* In contrast, claim 1 of the Richardson invention required a "spring means having a first end pivotally secured to said frame." *Id.* The jury in the district court found that Downs' failed to disclose each and every element of the Richardson claim and the Federal Circuit affirmed that finding. *Id.*

Turning to the instant application, Cheng merely discloses sending the credit card information, street address, etc. from one server to another. A review of Cheng reveals that Cheng is silent regarding generating credit card information, street address, telephone number, etc. Further, Cheng is silent regarding using the credit card information, street address, etc. to obtain identity assertion information, which

includes data associated with the user. Cheng, at best, discloses that sending personal data from one server to another across a network may be a violation of privacy law.

Just as in Richardson, where a spring element pivotally attached to a frame was not found to be anticipated by a spring element rigidly attached to a frame, the fact that Cheng discloses sending personal information from one server to another, where the personal information is equated to the first artifact, is not enough to anticipate generating the first artifact and using the first artifact to obtain identity assertion information. In view of the above, the complete identical claimed invention is not disclosed by the prior art. Thus, in view of *Richardson*, Cheng fails to anticipate the claimed invention.

2. Cheng fails to disclose verifying the validity of the first artifact upon receipt from the second application.

Variations of this argument were presented in the responses filed on February 26, 2008, June 27, 2008, and January 2, 2009. The Examiner erroneously contends that Cheng discloses verifying the validity of the first artifact upon receipt from the second application in col. 6, ll. 53-59. *See* Final Rejection p. 6. The cited section of Cheng discloses that when a request is sent to the first network device, such as a multiple domain, single sign on (MDSSO) server, the MDSSO server generates

an MDSSO cookie and sends the cookie back to the user device. *See* Cheng, col. 6, ll. 53-64. As described above, the Examiner also finds that the credit card information, street address, etc. is identical to the first artifact.

In *Net MoneyIN*, the district court found that all the elements of the claim were disclosed by the prior art and noted that because a simple combination was all that was required to produce the system, disclosure of linking the elements together was not required. The United States court of Appeals for the Federal Circuit overruled the district court, noting that "[b]ecause the hallmark of anticipation is prior invention, the prior art reference – in order to anticipate under 35 U.S.C. §102 – must not only disclose all the elements of the claim within the four corners or the document, but must also disclose those elements arranged as in the claim." *Net MoneyIN Inc. v. VeriSign, Inc.*, 2008 WL 4614511 (Fed. Cir. 2008).

In the instant case, the Examiner has relied on the personal information of Cheng as disclosing the first artifact in one limitation and has relied on the cookie of Cheng as disclosing the first artifact in another limitation. However, in view of *Net MoneyIN*, in order for Cheng to anticipate claim 27, Cheng must disclose the elements in the same arrangement as in the claim. Thus, in view of *Net MoneyIN*, the first artifact that is generated and associated with the identity assertion information must be the same first artifact whose validity is verified. Accordingly, in Cheng,

either i) the cookie must also be associated with the identity assertion information, and used to obtain the identity assertion information, or ii) the personal information (credit card information, street address, etc.) must be verified for validity. A review of Cheng reveals that Cheng fails to disclose either of these requirements. Accordingly, all of the elements of independent claim 27 are not arranged in the same way in Cheng. Thus, in view of *Net MoneyIN*, Cheng fails to anticipate claim 27.

3. Cheng fails to disclose rendering the first artifact invalid for future use by any of the plurality of applications

This argument has not been previously presented. Even considering, *arguendo*, that the cookie of Cheng anticipates the first artifact of the claimed invention, the Examiner's argument is still flawed. Cheng discloses an authentication front-end configured to receive a request to access a protected URL, where the request may contain a cookie. *See* Cheng col. 6, ll. 38-48. After authentication, a cookie is sent back to the user with redirect instructions to the protected URL that the user initially requested. The user may then use this cookie to access other servers within the domain. Accordingly, the cookie of Cheng is (i) maintained by the user (or more specifically in the end user device); (ii) the cookie may be reused to access different servers; and (iii) the cookie is used to directly authenticate the user to the server.

"Unless the steps of a method actually recite an order, the steps are not ordinarily construed to require one. However, such a result can ensue when the method steps implicitly require that they be performed in the order written." *Interactive Gift Express, Inc. v. Compuserve Inc.*, 256 F.3d 1323, 1342-43, 59 USPQ2d at 1416 (Fed. Cir. 2001); *Altiris, Inc. v. Symantic Corp.*, 318 F.3d 1363, 65 U.S.P.Q.2d (BNA) 1865 (Fed. Cir. 2003).

Appellants assert that the limitations of claim 27 *implicitly require* that they be performed in the order written, as evidenced by the fact that each limitation after the first relies on subject matter introduced in the previous limitation. Specifically, the fourth limitation describes generating a first artifact. The eighth limitation describes using the first artifact to receive identity assertion information. The tenth limitation describes rendering the first artifact invalid for future use by the plurality of applications. The eleventh limitation describes receiving a request for a second artifact from the second application. This process *clearly* delineates an order, and any deviation from that order without changing the subject matter of the limitations renders the final result different than that of claim 27 as it is written. Accordingly, the claimed invention requires that the first artifact is invalidated after a first use.

Cheng fails to disclose invalidating a first artifact after a first use. At best, the cookie in Cheng may have an expiry date (*see, e.g.*, Cheng col. 7, ll. 9-10). However,

a cookie that expires at an expiry date and a cookie that expires after a first use are not the same. Specifically, merely providing an expiry date for a cookie does not prohibit that cookie from being used more than once before the expiry date.

Further, as described above, *Richardson* requires that "[t]he identical invention must be shown in as complete detail as is contained in the claim." *Richardson* at 1236. Accordingly, as required by *Richardson*, the identical first artifact, which is invalidated after a single use, is not shown by Cheng.

Further, the artifacts themselves do not authenticate a user to an application in the claimed invention; rather, the artifact is used to obtain the identity assertion information that is used to authenticate the user to the application. The cookie in Cheng is not used to obtain any sort of information required for authentication, as the cookie *itself* is provided for the purpose of authenticating the user. Further, a review of Cheng reveals that Cheng is silent regarding any device that meets all the requirements of the first artifact. For at least these reasons, Cheng fails to disclose verifying the validity of the first artifact upon receipt from the second application.

4. Conclusion

In view of the above, the Examiner has clearly failed to show that claim 27 is anticipated by Cheng. Further, independent claims 34 and 41 include similar

limitations to claim 27 and, thus, are also not anticipated by Cheng for at least the same reasons. Accordingly, claims 27, 34, and 41 are allowable over Cheng. Further, claims 28-31, 33, 35, 37-38, 40, 42-45, and 47 depend from the independent claims and, thus, are also allowable over Cheng for at least the same reasons.

B. Claim 32

In this Appeal, the Appellants further argue that claims 32, 36, 39, and 46 are patentable under 35 U.S.C. § 103(a) over Cheng and Botz, viewed separately or in combination, for at least the reasons stated below.

Variations of this argument were presented in the responses filed on February 26, 2008, June 27, 2008, and January 2, 2009.

Claims 32, 36, and 46 depend on independent claims 27, 34, and 41 respectively. As discussed above, Cheng fails to teach or suggest all the limitations of amended independent claims 27, 34, and 41. Further, Botz fails to teach or suggest that which Cheng lacks. This is evidenced by the fact that Botz is only relied upon to teach SAML and that the identity assertion information is stored in the identity service provider. *See* Office Action mailed March 27, 2008, p. 7.

In view of the above, the Examiner has failed to show the presence of all elements in the prior art and thereby has failed to satisfied the requirements of *KSR*

International Co., which requires that the Examiner "articulate the following: (1) a finding that the prior art included each element claimed, although not necessarily in a single prior art reference, with the only difference between the claimed invention and the prior art being the lack of actual combination of the elements in a single prior art reference; ..." MPEP § 2143(A) citing *KSR International Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1739, 75 U.S.L.W. 4289 (2007). Accordingly, the Examiner has failed to show sufficient evidence of *prima facie* obviousness.

In view of the above, as the Examiner has failed to show sufficient evidence for a *prima facie* to support prima facie obviousness, the Appellants have carried their burden in showing that the Examiner erred in finally rejecting the claims. *In re Kahn*, 441 F.3d 977, 985-986 (Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness") (emphasis in original) (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)); *see also* 37 C.F.R. § 41.37(c)(1)(vii).

Therefore, independent claims 27, 34, and 41 are patentable over Cheng and Botz, for at least the reasons given above. Claims 32, 36, 39, and 46 depend, directly or indirectly, from the independent claims and are patentable over Cheng and Botz for

at least the same reasons. Accordingly, the rejection is respectfully traversed and withdrawal is respectfully requested.

VII. CONCLUSION

In view of the above, the Examiner's contentions and the cited art do not support the rejection of claims 27-31, 33-35, 37-38, 40-45, and 47 under 35 U.S.C. § 102(e). Further, the Examiner's contentions and the cited art do not support the rejection of claims 32, 36, 39, and 46 under 35 U.S.C. § 103(a). Accordingly, a favorable decision from the Board is respectfully requested.

Dated: February 6, 2009

Respectfully submitted,

By /Robert P. Lord/

Robert P. Lord
Registration No.: 46,479
OSHA · LIANG LLP
909 Fannin Street, Suite 3500
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)

APPENDIX A - CLAIMS

1. – 26. (Cancelled)

27.(Rejected) A method for managing access to a plurality of applications using a central server, comprising:

receiving a user name and a user password of a user from a first application;

authenticating the user using the user name and password;

generating, in response to the successful authentication, identity assertion information comprising information associated with the user for use by a plurality of applications to authenticate the user;

generating a first artifact associated with the identity assertion information, wherein the first artifact is used to obtain the identity assertion information;

sending the first artifact to the first application;

receiving the first artifact and a request for the identity assertion information from a second application, wherein the second application receives the first artifact from the first application;

verifying the validity of the first artifact upon receipt from the second application;

retrieving, after successful validation of the first artifact, the identity assertion information for the user using the first artifact;

sending the identity assertion information to the second application, wherein the second application uses the identity assertion information to authorize the user to access the second application;

rendering the first artifact invalid for future use by any of the plurality of applications;

receiving a request for a second artifact from the second application; and

providing the second artifact associated with the identity assertion information, wherein the second artifact is used to obtain the identity assertion information,

wherein the first application and the second application are members of the plurality of applications.

28.(Rejected) The method of claim 27, further comprising:

receiving the second artifact and request for the identity assertion information from a third application, wherein the third application receives the second artifact from the second application;

verifying the validity of the second artifact upon receipt from the third application;

retrieving, upon successful validation, the identity assertion information for the user using the second artifact;

sending the identity assertion information to the third application, wherein the third application uses the identity assertion information to authorize the user to access the third application;

rendering the second artifact invalid for future use by any of the plurality of applications;

receiving a request for a third artifact from the second application; and

providing the third artifact associated with the identity assertion information, wherein the third artifact is used to obtain the identity assertion information,

wherein the third application is a member of the plurality of applications.

29.(Rejected) The method of claim 27, wherein the identity assertion information is stored in the central server.

30.(Rejected) The method of claim 27, wherein the first artifact comprises a type code, a source identification, and an assertion identification.

31.(Rejected) The method of claim 30, wherein the first artifact further comprises a server identification.

32.(Rejected) The method of claim 27, wherein the identity assertion information is generated in accordance with a Security Assertions Markup Language (SAML) standard.

33.(Rejected) The method of claim 27, wherein the user name and the user password are obtained by the first application from a web browser.

34.(Rejected) A system for managing access to a plurality of applications comprising:

a processor; and

an identity service provider executing on the processor, configured to:

receive a user name and a user password of a user from a first application;

authenticate the user using the user name and password;

generate, in response to the successful authentication, identity assertion information comprising information associated with the user for use by a plurality of applications to authenticate the user;

generate a first artifact associated with the identity assertion information, wherein the first artifact is used to obtain the identity assertion information;

send the first artifact to the first application;

receive the first artifact and a request for the identity assertion information from a second application, wherein the second application receives the first artifact from the first application;

verify the validity of the first artifact upon receipt from the second application;

retrieve, after successful validation of the first artifact, the identity assertion information for the user using the first artifact;

send the identity assertion information to the second application, wherein the second application uses the identity assertion information to authorize the user to access the second application;

render the first artifact invalid for future use by any of the plurality of applications;

receive a request for a second artifact from the second application; and

provide the second artifact associated with the identity assertion information, wherein the second artifact is used to obtain the identity assertion information,

wherein the first application and the second application are members of the plurality of applications.

35.(Rejected) The system of claim 34, wherein the identity service provided is further configured to:

receive the second artifact and request for the identity assertion information from a third application, wherein the third application receives the second artifact from the second application;

verify the validity of the second artifact upon receipt from the third application;

retrieve, upon successful validation, the identity assertion information for the user using the second artifact;

render the second artifact invalid for future use by any of the plurality of applications;

receive a request for a third artifact from the second application; and

provide the third artifact associated with the identity assertion information, wherein the third artifact is used to obtain the identity assertion information,

wherein the third application is a member of the plurality of applications.

36.(Rejected) The system of claim 34, wherein the identity assertion information is stored in the identity service provider.

37.(Rejected) The system of claim 34, wherein the first artifact comprises a type code, a source identification, and an assertion identification.

38.(Rejected) The system of claim 37, wherein the first artifact further comprises a server identification.

39.(Rejected) The system of claim 34, wherein the identity assertion information is generated in accordance with a Security Assertions Markup Language (SAML) standard.

40.(Rejected) The system of claim 34, wherein the user name and the user password are obtained by the first application from a web browser.

41.(Rejected) A computer readable memory comprising program instructions that, when executed by a processor, implement a method managing access to a plurality of applications using a central server, the method comprising:

receiving a user name and a user password of a user from a first application;

authenticating the user using the user name and password;

generating, in response to the successful authentication, identity assertion information comprising information associated with the user for use by a plurality of applications to authenticate the user;

generating a first artifact associated with the identity assertion information, wherein the first artifact is used to obtain the identity assertion information;

sending the first artifact to the first application;

receiving the first artifact and a request for the identity assertion information from a second application, wherein the second application receives the first artifact from the first application;

verifying the validity of the first artifact upon receipt from the second application;

retrieving, after successful validation of the first artifact, the identity assertion information for the user using the first artifact;

sending the identity assertion information to the second application, wherein the second application uses the identity assertion information to authorize the user to access the second application;

rendering the first artifact invalid for future use by any of the plurality of applications;

receiving a request for a second artifact from the second application; and

providing the second artifact associated with the identity assertion information, wherein the second artifact is used to obtain the identity assertion information,

wherein the first application and the second application are members of the plurality of applications

42.(Rejected) The computer readable memory of claim 41, where the method further comprises:

receiving the second artifact and request for the identity assertion information from a third application, wherein the third application receives the second artifact from the second application;

verifying the validity of the second artifact upon receipt from the third application;

retrieving, upon successful validation, the identity assertion information for the user using the second artifact;

sending the identity assertion information to the third application, wherein the third application uses the identity assertion information to authorize the user to access the third application;

rendering the second artifact invalid for future use by any of the plurality of applications;

receiving a request for a third artifact from the second application; and

providing the third artifact associated with the identity assertion information,

wherein the third artifact is used to obtain the identity assertion information,

wherein the third application is a member of the plurality of applications.

43. (Rejected) The computer readable memory of claim 41, wherein the identity assertion information is stored in the central server.

44. (Rejected) The computer readable memory of claim 41, wherein the first artifact comprises a type code, a source identification, and an assertion identification.

45. (Rejected) The computer readable memory of claim 44, wherein the first artifact further comprises a server identification.

46. (Rejected) The computer readable memory of claim 41, wherein the identity assertion information is generated in accordance with a Security Assertions Markup Language (SAML) standard.

47. (Rejected) The computer readable memory of claim 41, wherein the user name and the user password are obtained by the first application from a web browser.

APPENDIX B – CLAIM SUPPORT AND DRAWING ANALYSIS

The following references to the specification and figures should not be construed as the only locations in the specification and figures for which support for the corresponding claim limitations may be found.

27. A method for managing access to a plurality of applications using a central server, comprising:

receiving a user name and a user password of a user from a first application; **{p. 20 lines 19-25; Fig. 5, 2}**

authenticating the user using the user name and password; **{p. 20 line 21 – p. 21 line 3; Fig. 5, 510}**

generating, in response to the successful authentication, identity assertion information comprising information associated with the user for use by a plurality of applications to authenticate the user; **{p. 20 lines 9-20; Fig. 5, 550}**

generating a first artifact associated with the identity assertion information, wherein the first artifact is used to obtain the identity assertion information; **{p. 35 lines 6-8; Fig. 5, 555}**

sending the first artifact to the first application; **{p. 35 lines 10-11; Fig. 5, 4}**

receiving the first artifact and a request for the identity assertion information from a second application, wherein the second application receives the first artifact from the first application; **{p. 35 lines 19-25; Fig. 5, 6}**

verifying the validity of the first artifact upon receipt from the second application; **{p. 36 lines 8-16; Fig. 5, 510}**

retrieving, after successful validation of the first artifact, the identity assertion information for the user using the first artifact; **{p. 36 lines 11-16; Fig. 5, 550}**

sending the identity assertion information to the second application, wherein the second application uses the identity assertion information to authorize the user to access the second application; **{p. 36 lines 11-16; Fig. 5, 7}**

rendering the first artifact invalid for future use by any of the plurality of applications; **{p. 37 lines 4-6; Fig. 5, 555}**

receiving a request for a second artifact from the second application; **{p. 37 lines 1-8; Fig. 5, 8}** and

providing the second artifact associated with the identity assertion information, wherein the second artifact is used to obtain the identity assertion information, **{p. 37 lines 20-24; Fig. 5, 9}**

wherein the first application and the second application are members of the plurality of applications. **{p. 37 lines 4-6; Fig. 5, 520, 530}**

32. The method of claim 27, wherein the identity assertion information is generated in accordance with a Security Assertions Markup Language (SAML) standard. **{p. 22 lines 20-25; Fig. 2, 210}**

34. A system for managing access to a plurality of applications comprising:

a processor; **{p. 9 lines 15-17; Fig. 5, 555}** and

an identity service provider executing on the processor, **{p. 33 lines 20-24; Fig. 5, 510}** configured to:

receive a user name and a user password of a user from a first application; **{p. 20 lines 19-25; Fig. 5, 2}**

authenticate the user using the user name and password; **{p. 20 line 21 – p. 21 line 3; Fig. 5, 510}**

generate, in response to the successful authentication, identity assertion information comprising information associated with the user for use by a plurality of applications to authenticate the user; **{p. 20 lines 9-20; Fig. 5, 550}**

generate a first artifact associated with the identity assertion information, wherein the first artifact is used to obtain the identity assertion information; **{p. 35 lines 6-8; Fig. 5, 555}**

send the first artifact to the first application; **{p. 35 lines 10-11; Fig. 5, 4}**

receive the first artifact and a request for the identity assertion information from a second application, wherein the second application receives the first artifact from the first application; **{p. 35 lines 19-25; Fig. 5, 6}**

verify the validity of the first artifact upon receipt from the second application; **{p. 36 lines 8-16; Fig. 5, 510}**

retrieve, after successful validation of the first artifact, the identity assertion information for the user using the first artifact; **{p. 36 lines 11-16; Fig. 5, 550}**

send the identity assertion information to the second application, wherein the second application uses the identity assertion information to authorize the user to access the second application; **{p. 36 lines 11-16; Fig. 5, 7}**

render the first artifact invalid for future use by any of the plurality of applications; **{p. 37 lines 4-6; Fig. 5, 555}**

receive a request for a second artifact from the second application; **{p. 37 lines 1-8; Fig. 5, 8}** and

provide the second artifact associated with the identity assertion information, wherein the second artifact is used to obtain the identity assertion information, **{p. 37 lines 20-24; Fig. 5, 9}**

wherein the first application and the second application are members of the plurality of applications. **{p. 37 lines 4-6; Fig. 5, 520, 530}**

41. A computer readable memory comprising program instructions that, when executed by a processor, implement a method managing access to a plurality of applications using a central server, the method comprising:

receiving a user name and a user password of a user from a first application; **{p. 20 lines 19-25; Fig. 5, 2}**

authenticating the user using the user name and password; **{p. 20 line 21 – p. 21 line 3; Fig. 5, 510}**

generating, in response to the successful authentication, identity assertion information comprising information associated with the user for use by a plurality of applications to authenticate the user; **{p. 20 lines 9-20; Fig. 5, 550}**

generating a first artifact associated with the identity assertion information, wherein the first artifact is used to obtain the identity assertion information; **{p. 35 lines 10-11; Fig. 5, 4}**

sending the first artifact to the first application; **{p. 35 lines 6-8; Fig. 5, 555}**

receiving the first artifact and a request for the identity assertion information from a second application, wherein the second application receives the first artifact from the first application; **{p. 35 lines 19-25; Fig. 5, 6}**

verifying the validity of the first artifact upon receipt from the second application; **{p. 36 lines 8-16; Fig. 5, 510}**

retrieving, after successful validation of the first artifact, the identity assertion information for the user using the first artifact; **{p. 36 lines 11-16; Fig. 5, 550}**

sending the identity assertion information to the second application, wherein the second application uses the identity assertion information to authorize the user to access the second application; **{p. 36 lines 11-16; Fig. 5, 7}**

rendering the first artifact invalid for future use by any of the plurality of applications; **{p. 37 lines 4-6; Fig. 5, 555}**

receiving a request for a second artifact from the second application; **{p. 37 lines 1-8; Fig. 5, 8}** and

providing the second artifact associated with the identity assertion information, wherein the second artifact is used to obtain the identity assertion information, **{p. 37 lines 20-24; Fig. 5, 9}**

wherein the first application and the second application are members of the plurality of applications. **{p. 37 lines 4-6; Fig. 5, 520, 530}**

APPENDIX C – MEANS OR STEP PLUS FUNCTION ANALYSIS

The pending claims do not include any claims that require means or step plus function analysis.

APPENDIX D – EVIDENCE

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the Examiner is being submitted.

APPENDIX E – RELATED CASES

No related proceedings are referenced in II. above, hence copies or decisions in related proceedings are not provided.